REMARKS

As a preliminary matter, counsel for Applicant first wishes to thank Examiner Klimach for taking the time to speak over the telephone regarding the claims in the current Office Action. Counsel for Applicant noted an oversight wherein the Office Action addressed claims 1-26, but not the remaining claims 27-42. Accordingly, this response does not discuss the merits of the rejections with respect to claims 27-42 in any detail. Examiner Klimach graciously apologized for the oversight, and agreed to make the next Office Action (if any) non-final.

The Examiner rejected claim 1 under 35 U.S.C. § 103(a) as being unpatentable over the patent to White in view of the article to Wey in further view of the article to Heikes. Applicant respectfully traverses the rejection. Claim 1 is directed to a recursive squaring circuit having a host processor, a co-processor, and one or more hardware circuits that may be used, for example, in cryptography applications. Both the host processor and the co-processor operate recursively to reduce respective starting integer values to reduced-length integer values and hardware length values, respectively. Further, the recursive processes on both processors interoperate with each other in that the starting integer values for the recursive process on the co-processor are the reduced-length integer values received from the recursive process on the host processor.

Respectfully, the rejections appear to be based on a collection of independent concepts pieced together using claim 1 as a blueprint. At least two of the cited references have nothing to do with recursion or recursive structures at all, and none of the references teach or suggest the either the host processor or the coprocessor as recited by claim 1. Finally, none of the references teach or suggest the interoperation between the host processor and the co-processor.

The White patent, for example, discloses a circuit that operates on different parts of a single starting value (i.e., a most significant part and a least significant part). However, as the Examiner readily admits, it fails to even mention recursion. Whatever White discloses, the

Examiner's admission necessarily means that this reference fails to teach or suggest at least two aspects of the invention as claimed. First, it means that White fails to teach or suggest both the host processor and the co-processor (both of which operate recursively to reduce their respective starting values). Second, it means that White fails to teach or suggest that the host processor provides recursively reduced length integer values to the co-processor (for further recursive reduction). The parallel circuit of White simply operates on different portions of a starting value concurrently.

Heikes has the same deficiencies as White. The Examiner cites Heikes for its teaching of a co-processor as part of a PA-RISC processor. However, this goes only to the physical location of the circuit. Heikes discloses nothing regarding recursive operations. The extent of the Heikes disclosure regards the specifics of a multiplier array on a math co-processor. It never mentions that the array, the co-processor, or the PA-RISC processor operates recursively, and not even the Examiner asserts that it does. Heikes fails to teach or suggest the claimed host processor and the claimed co-processor, as well as the claimed operational relationship between the two processors.

Finally, the Examiner attempts to add Wey's article for its teaching of a recursively operating multiplier circuit. However, scrutiny reveals that the Examiner's assertion -- that the circuit is a co-processor designed to recursively reduce starting values -- is based on an overstatement of what Wey actually discloses. Wey does not identify the disclosed circuit as a co-processor. Rather, Wey's circuit is a multiplier circuit that recursively partitions a multiplier and a multiplicand into a fixed number of groups having a fixed number of bits each. Even if the circuit of Wey could be construed as a co-processor, the values partitioned by the multiplier circuit are whole integers and not reduced length integer values produced recursively by a host processor. That is, Wey does not teach or suggest a host processor providing recursively reduced length values as starting values for further recursive length reduction by a co-

processor. Thus, Wey, like White and Heikes, fails to teach or suggest the host processor or the co-processor as recited by claim 1.

Therefore, none of the cited references, taken alone or in any combination, teach or suggest the invention of claim 1. As such, the §103 rejection necessarily fails as a matter of law. Additionally, the §103 rejection fails for other reasons. Specifically, the patent to White cannot be combined with either the article to Wey or to Heikes. The reason White uses a parallel circuit (as opposed to a recursive circuit) is to reduce the demand imposed on the limited memory resources associated with ROM devices. *E.g., White*, col. 2, ll. 23-25. However, this stated goal contradicts the use of a recursive process. Recursive processes, such as that of Wey, require a substantial amount of memory to store values and information (e.g., starting values, accumulated values, and addresses). This data is saved at each recursive step to ensure that it is available upon return to the calling function. Indeed, it is not surprising that White is silent on the subject of recursion.

Another reason is the Examiner's proffered motivation to combine White and Heikes. Both references already disclose some type of multiplier circuit that allows concurrent operations. As such, neither reference adds anything to the other when combined. In addition, nothing in either reference suggests that one circuit would or could provide the other with reduced length integer values. For at least these reasons, no one skilled in the art would be motivated to combine the cited references.

For the reasons stated above, the cited references fail to teach or suggest, alone or in combination, claim 1. Accordingly, Applicant respectfully requests the allowance of claim 1 and its dependent claims 2-8.

The Examiner also rejected claim 9 under 35 U.S.C. § 103(a) for the same reasons and in view of the same art as cited above for claim 1. Claim 9, however, recites subject matter similar to that recited by claim 1. Therefore, White, Wey, and Heikes, taken alone or in any

combination, fail to teach or suggest the invention of claim 9. Accordingly, Applicant respectfully requests the allowance of claim 9 and its dependent claims 10-16.

The Examiner also rejected claim 17 under 35 U.S.C. § 103(a) over White in view of Wey and Heikes. However, claim 17 recites that the host processor operates recursively (as noted above). At each recursive step, the host processor further randomly orders the ending integer values used by the co-processor. None of the references teach or suggest, alone or in combination, the recursively operating host processor, let alone the requisite random ordering at each recursive step. Notably, the Examiner never asserts that they do. Accordingly, none of the references, taken alone or in any combination, teach or suggest the invention of claim 17. As such, Applicant respectfully requests the allowance of claim 17 and its dependent claims 18-26.

Finally, as noted above, the Office Action does not explicitly reject any of claims 27-42. However, Applicant notes that each of the independent claims 27, 29, 31, and 33 patentbly define over the cited art for reasons similar to those stated above. Accordingly, Applicant respectfully requests the allowance of all pending claims 1-42.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: February 22, 2005

Stephen A. Herrera
Registration No.: 47,642

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844